Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 24 (2016) 896 – 903

Procedia Technology

International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015)

Analysis of Physical layer Security via Co-operative Communication in Internet of Things

Aparna K Nair[a] , Shaniba Asmi[b] , Dr.Gopakumar A[c]

[a]*PG scholar, Dept. of ECE, MES college of engg, Kuttippuram, 679573, India*
[b]*Associate Professor, Dept of ECE, MES college of engg, Kuttippuram, 679573, India*

Abstract

Co-operative communication in Internet of Things enable the co-existing heterogeneous wireless networks to co-operate with each other in order to facilitate network traffic, guarantee QoS requirements and to enable energy efficient secure communication even to most demanding users. Physical layer security approaches based on node cooperation promise secure communication even in the presence of an eavesdropper. The three main co-operative schemes that help in improving physical layer (PHY) security via co-operative communication are decode-and-forward (DF), amplify-and-forward (AF) and co-operative jamming (CJ). This work mainly focuses on the performance analysis of PHY layer security via two co-operative schemes (DF and AF) by taking all main fading phenomenon's like path loss, phase fading and shadow fading into consideration. Also a method has been discussed for enhancing the secrecy rate by using two heuristic algorithms: "hill-climbing" and "random-search".

Peer-review under responsibility of the organizing committee of ICETEST – 2015

*Keywords:*Internet of Things; Physical layer security; Co-operative communication

1. Introduction

The Internet of Things (IoT) represents a vision in which the physical items are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. Security is therefore very essential, since everything is connected to Internet and these things have a capacity to connect themselves [1]. A secure IoT platform can be obtained by integrating the co-operative communication in case of wireless sensor networks to that of Internet of things. In a cooperative communication system, each wireless user is assumed to transmit data as well as act as a cooperative agent for another user. This co-operation promises low power, low cost object monitoring and networking. Cooperative communication in IoT enable the co-existing heterogeneous wireless networks and mobile terminals evolve so as to co-operate with each other in order to facilitate network traffic and guarantee QoS requirements even to most demanding

*Aparna K Nair. Tel.: +91-9446361219, *E-mail address:* aparna1161621@gmail.com

Peer-review under responsibility of the organizing committee of ICETEST – 2015
doi:10.1016/j.protcy.2016.05.162

users. Co-operative communication put forwards certain advantages to IoT platform like energy efficiency, scalability, reliability, robustness and self healing.

Physical layer (PHY) security gathers prime importance as it is responsible for frequency selection, modulation, and encryption and so on. Since it's of low power and low storage capability, higher security options like cryptographic techniques and public key encryption mechanisms are slightly inapplicable on PHY layer. Physical layer security without relying on private keys was pioneered by Wyner in [2] by introducing a wiretap channel. He established that it's possible to have secure communication when the source-destination channel is stronger than the source-wiretap channel. Later on these works were extended in [3] where the term "secrecy capacity" was introduced to describe whether the communication is secure or not. Secrecy rate is the rate at which information can be secretly transmitted from source to destination. The PHY layer security approaches based on single antenna systems were easily hampered by the channel conditions like absent feedback and this can be overcome by multiple antenna systems(MIMO,MISO,SIMO)[4][5]. Since the cost and size limitations of multiple antenna systems made it unavailable at the network node, "node cooperation" was evolved where a single antenna can enjoy the benefits of multiple antenna. Relay nodes, relay channels and its extension forms the basis of the co-operative communication scenario. Relay nodes are simply the intermediate nodes present in between the source and the destination nodes that allow either passive or active cooperation. In this paper, a source communicates with a destination with the help of multiple relays in the presence of one or more eavesdroppers. The three main cooperative schemes that enable cooperative communication are decode- and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ). Our discussion is limited only to decode- and-forward (DF) and amplify-and-forward (AF) schemes.

1.1. Related works

The three cooperative schemes (DF,AF,CJ) in the absence and presence of an eavesdropper were studied in [6]-[10]. Decode-and-forward(DF) and amplify and forward(AF) co-operative schemes with an objective of secrecy capacity maximization or transmit power minimization were studied in [6] and [7]. In co-operative jamming (CJ), secure communication takes place by confounding the eavesdropper by sending a jamming signal [8]. Relay nodes play an important role in cooperative communication. Relay node can perform a dual role; either by helping the eavesdropper or the source-destination link. A four-node system model with the rate-equivocation region and the applicable scenarios of cooperation were studied in [11].Secure communication of a source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers for three cooperative schemes (DF, AF, CJ) were studied in [12], where the objective was achievable secrecy rate maximization and transmit power minimization.

2. System model

System models and initial conditions considered here are as similar as that of [12]. A wireless network model with a source-destination pair, N trusted relays and J eavesdroppers $(J \leq 1)$ are considered. Assume that the global CSE is available. The eavesdropper channel, source encoding schemes, decoding schemes and cooperative protocol are considered to be public; only source message is assumed to be confidential. Here, the discussion is limited to two main cooperative schemes: decode-and-forward (DF) and amplify-and-forward (AF). The notations that are used are tabulated and shown in Table I.

Table I: Notations

Symbol	Description
$(.)^*$	Conjugate
$(.)^T$	Transpose
$(.)^\dagger$	Conjugate transpose
I_M	Identity matrix of size $M \times N$
$diag\{a\}$	Diagonal matrix with the elements of the vector a along its diagonal.
$\|a\|$	2-norm of the vector a.
$0_{M \times N}$	All-zero matrix of size $M \times N$.
$log(.)$	Base-2 logarithm
h_{SD}^*	Baseband complex channel gain between source and destination
h_{SE}^*	Channel vector$(J \times 1)$ between source and J eavesdroppers
h_{SR}^*	Channel vector$(N \times 1)$ between source and N relays
h_{RD}^*	Channel vector$(N \times 1)$ between N relays and destination
H_{RE}^*	Channel matrix$(N \times J)$ between N relays and J eavesdroppers

2.1. Decode-and-forward (DF)

There are two main stages in DF. Source broadcasts its encoded symbols to its trusted relays using the first transmission slot in Stage 1. When transmitting the symbol x, the received signals at the N relays are given by,

$$y_r = \sqrt{P_s} h_{SR}^* x + n_r \tag{1}$$

where P_s is the transmit power of source and n_r is the noise vector at relays.
In Stage 2, all the trusted relays that successfully decode the message, re-encode the message and cooperatively transmit the re-encoded symbols to the destination by using the second transmission slot. Each relay transmits a weighted version of the re-encoded symbol. When transmitting the symbol $\tilde{x}$, the received signal at the destination is given by,

$$y_d = h_{RD}^\dagger w \tilde{x} + n_d \tag{2}$$

while the received signal at the eavesdroppers is expressed in vector form as,

$$y_e = H_{RE}^\dagger w \tilde{x} + n_e \tag{3}$$

The transmit power budget for Stage 2 is considered to be $P - P_s$ where P is the total power for transmitting one symbol and P_s is the transmit power of source.

2.2. Amplify-and-forward (AF)

AF is also a two-stage scheme as that of DF. Stage 1 is the same for both AF and DF, except that the transmit power can be different. The trusted relays forward the signals that are received during Stage 1 to the destination, using the second transmission slot in Stage 2. That is, each relay transmits a weighted version of the noisy signal that they received during Stage 1. The transmitted signals of all relays are denoted by the product of $diag\{w\}y_r$ where w is the weight vector and y_r is given by (1). The received signal at the destination is given by,

$$y_d = \sqrt{P_s} h_{RD}^\dagger diag\{w\} h_{SR}^* x + h_{RD}^\dagger diag\{w\} n_r + n_d \tag{4}$$

The received signals at the eavesdroppers, in a vector form, is denoted by,

$$y_e = \sqrt{P_s} H_{RE}^\dagger diag\{w\} h_{SR}^* x + H_{RE}^\dagger diag\{w\} n_r + n_e \tag{5}$$

3. Effect of Fading in PHY layer security

The effect of different fading phenomenon's like path loss, shadowing and phase fading in PHY layer security is expressed in terms of channel gain and is shown below. The channel gain between any two nodes when path loss attenuation alone is considered is generally expressed as,

$$h_{ij} = \left(d_{ij}\right)^{-\gamma} \tag{6}$$

where γ is the path loss exponent and d_{ij} is the distance between the two nodes i and j . h_{ij} is the channel gain

between two nodes i and j. When phase fading is also considered, the channel gain between any two nodes can be expressed as

$$h_{ij} = \left(d_{ij}\right)^{-\gamma} \, \mathrm{e}^{\mathrm{j}\theta} \tag{7}$$

where θ is the random phase uniformly distributed in the $[0-2\pi]$ interval.

Incorporating shadowing attenuation along with the path loss, the channel gain can be formulated in terms of logarithmic model as

$$h_{ij} = -10\gamma \log(d_{ij}) + \mathrm{X}_{\sigma} \tag{8}$$

And logarithmic model can be expressed as,

$$h_{ij} = \left(d_{ij}\right)^{-\gamma} 10^{-\mathrm{X}_{\sigma}/10} \mathrm{e}^{\mathrm{j}\theta} \tag{9}$$

where X_{σ} is the Gaussian random variable with zero mean and standard deviation σ. X_{σ} is expressed in log-normal distribution. In case of microcells the σ varies in between 6-8dB and in case of macro-cells, σ is normally 3dB. Therefore by considering the shadowing attenuation in addition to path loss and phase fading, the analysis of physical layer security via two co-operative schemes (DF and AF) is done as follows.

3.1. Decode and forward

Here assume that all N relays successfully decode the message and the relays use same codeword's as that of source. The rate at the destination, incorporating the effects of shadowing along with path loss and phase fading is given by,

$$R_d = \frac{1}{2}\log\left(\alpha + \frac{w^{\dagger} R_{RD} w}{\sigma^2}\right) \tag{10}$$

where $R_{RD} = h_{RD} h_{RD}^{\dagger}$ and $\alpha = 1 + P_s \left|h_{SD}\right|^2 / \sigma^2$.

The strategy to achieve the capacity in (10) is maximal ratio combining(MRC). $P_s \left|h_{SD}\right|^2 / \sigma^2$ is the received signal-to-noise ratio (SNR) in Stage 1 at the destination and the scalar factor $1/2$ describes the two time units that are required in two stages. The rate at the eavesdroppers is are also obtained in a similar way .

1) Relay weight optimization

One eavesdropper: In the case of one eavesdropper, the rate at the eavesdropper obtained from [12] is given by,

$$R_e = \frac{1}{2}\log\left(\beta + \frac{w^{\dagger} R_{RE} w}{\sigma^2}\right) \tag{11}$$

where $R_{RD} = h_{RD} h_{RD}^{\dagger}$ and $\beta = 1 + P_s \left|h_{SE}\right|^2 / \sigma^2$

Then the achievable secrecy rate can be written as per [12] as,

$$R_s(w, P_s) = \frac{1}{2}\log\left(\frac{\alpha\sigma^2 + w^{\dagger} R_{RD} w}{\beta\sigma^2 + w^{\dagger} R_{RE} w}\right) \tag{12}$$

Multiple eavesdroppers: In the case of multiple eavesdroppers, by nulling out the signals at the eavesdroppers in Stage 2, the achievable secrecy rate obtained as per [12] is given as,

$$R_s(w,P_s)=\frac{1}{2}\log\left(\alpha+\frac{w^{\dagger}R_{RD}w}{\sigma^2}\right)-\log\left(\max_j(\beta_j)\right) \tag{13}$$

where $\beta_j=1+P_s|h_{SE}(j)|^2/\sigma^2$ and $h_{SE}(j)$ denotes the i^{th} element of vector h_{SE}

2) Selection of source power

The close form solution for finding source power in the case of multiple eavesdroppers is derived in [12].The secrecy rate obtained in the case of one eavesdropper can be improved by using two heuristic iterative algorithms namely "hill-climbing" and "random search" [12].

1. **Hill-climbing algorithm**

Step 0) Choose an initial value of P_s, e.g., the solution for the case of multiple eavesdroppers. Compute the corresponding unit-norm weight vector w. Step 1) Fix w, and vary P_s and find the corresponding secrecy rate. Update P_s if the varied P_s yields a higher secrecy rate. Step 2) Fix P_s and vary w. Update w if the varied w yields higher secrecy rate. Step 3) Repeat steps 1) and 2) until the secrecy rate cannot be improved further, or a predefined number of iterations has been reached.

2. **Random-search algorithm**

Step 0) Initialize the algorithm by setting an initial value of P_s, e.g., the solution for the case of multiple eavesdroppers. Step 1) Vary P_s and w and find the secrecy rate correspondingly. Update the weight vector w ,if the varied w yields to higher secrecy rate. Update the power P_s if the varied P_s yields to higher secrecy rate .Otherwise, keep the same power. Step 2) Repeat Step 1) until a predefined number of iterations is reached or the secrecy rate cannot be improved further.

3.2. Amplify and forward

In the case of AF, by incorporating the effects of these fading phenomenon's the rate at destination can be obtained as per [12] and is given by,

$$R_d=\frac{1}{2}\log\left(\alpha+\frac{w^{\dagger}R_a w}{\left(w^{\dagger}Uw+1\right)\sigma^2}\right) \tag{14}$$

where

$$a=\sqrt{P_s}\,diag\{h_{SR}\}h_{RD}$$
$$R_a=aa^{\dagger}$$
$$U=diag\{h_{RD}^{*}\}$$

The rate at the eavesdropper is given by ,

$$R_e = \frac{1}{2}\log\left(\beta + \frac{w^{\dagger}R_b w}{\left(w^{\dagger}Vw+1\right)\sigma^2}\right) \tag{15}$$

where $b = \sqrt{P_s}\,diag\{h_{SR}\}H_{RE}$, $R_b = bb^{\dagger}$ and $V = diag\{h_{RE}^{*}\}diag\{h_{RE}\}$

The achievable secrecy rate for one eavesdropper can be written as per [12] as,

$$R_s(w,P_s) = \frac{1}{2}\log\left(\alpha + \frac{w^{\dagger}R_a w}{\left(w^{\dagger}Uw+1\right)\sigma^2}\right) - \frac{1}{2}\log\left(\alpha + \frac{w^{\dagger}R_a w}{\left(w^{\dagger}Uw+1\right)\sigma^2}\right) \tag{16}$$

4. Numerical Results

The performance of the existing system design for improving the PHY layer security via two co-operative schemes (DF and AF) are shown in Fig. 1. Here channel gain between any two nodes depends only on path loss and phase fading attenuation. The source and destination locations are fixed at two-dimensional coordinates (0,0) and (50,0) respectively (unit: meters).

Fixing the relay location at (25,0), the position of eavesdroppers were varied from (30,0) to (90,0) and the achievable secrecy rate were plotted by performing Monte Carlo experiments consisting of 1000 independent trials to obtain the average results. The number of relays is $N = 3$ and number of eavesdroppers is taken as $J = 2$. It can be seen from Fig. 1 that, when eavesdroppers move away from the source, the secrecy rate increases for DF and AF, since the received signal power at the eavesdroppers decreases. Also it can be understood that DF does not necessarily perform better than AF, since the optimal source power could be different for DF and AF.

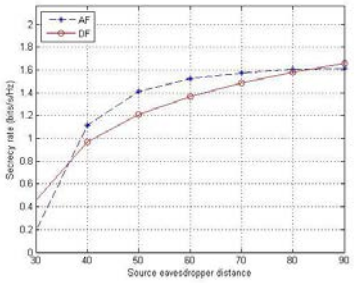

Fig. 1. Secrecy rate Vs source-eavesdropper distance.

To have a clear view on PHY layer security, shadow fading was also incorporated along with path loss and phase fading and then secrecy rate was plotted correspondingly. It can be seen that when obstacles where added in the transmission path, secrecy rate reduced gradually for the two cooperative schemes (DF and AF). Fig. 2 (a) and (b) shows the comparison of two cooperative schemes with and without adding the effect of shadow fading. Here the channel gain between two nodes can be formulated based the equation (9) formulated above. The path loss exponent was taken to be 3.5 and shadowing was

expressed in terms of the Gaussian random variable log normally distributed with zero mean and standard deviation 8dB. The noise power is taken to be-60dBm.

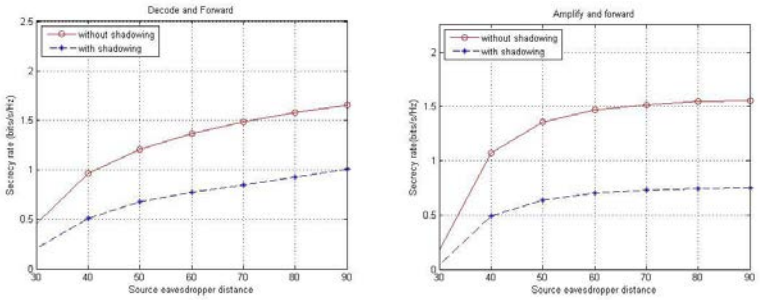

Fig. 2. Secrecy rate Vs source-eavesdropper distance with number of relays N=3and J =2 for (a) DF; (b) AF

Now the secrecy rate obtained via DF and AF can be enhanced using "hill-climbing" and "random-search" algorithms. Fig. 3. (a) and (b) shows that while using these algorithms, by optimizing both weight vector and source power, better secrecy rate can be achieved. It was found that DF performed slightly better than AF when eavesdropper was placed at a farther distance from source.

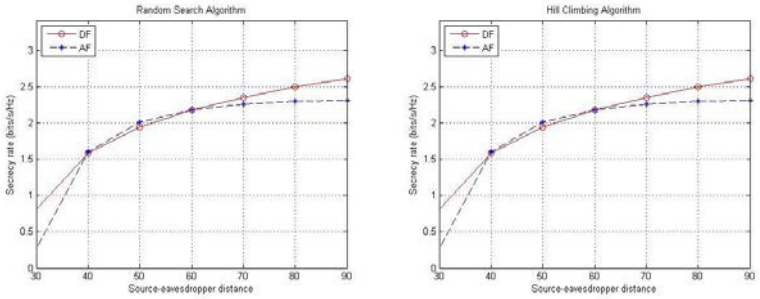

Fig. 3. Secrecy rate obtained after applying (a) Random-search algorithm; (b) Hill climbing algorithm

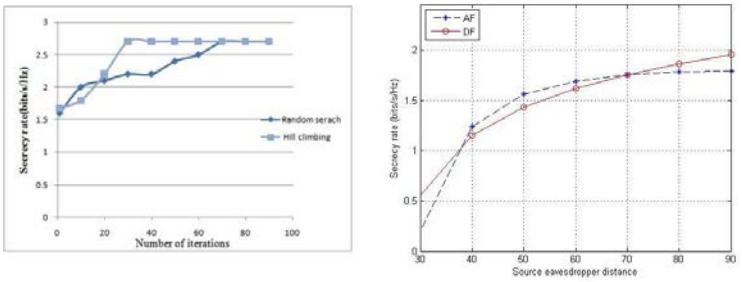

Fig. 4. (a) Secrecy rate Vs number of iterations; (b) Secrecy rate obtained by incorporating shadowing effect and further optimized by an iterative algorithm.

Both these algorithms can be used either to obtain global optimal solution or local optimal solution. Random search algorithm is considered to be the best suited for local-optimal cases and hill climbing is considered to be the best suited for global optimal cases. It was found that random search algorithm completes its global search with large number of iterations

and more execution time. On the other hand, hill-climbing algorithm can be used for global optimal solutions for obtaining a better secrecy rate with less number of iterations and less execution time when compared to random search. But since all possible combinations of weight vector and source power is been checked, random-search algorithm is considered to be accurate one when compared to hill-climbing. In Fig. 4 (a), the comparison of these algorithms can be seen based on number of iterations. Hill-climbing completed its global search and converges to a better secrecy rate with less number of iterations when compared to random-search. It was observed that when secrecy rate obtained under all fading phenomenon's (path loss, shadow fading, phase fading) was again optimized by these heuristic algorithms a better secrecy rate could be achieved as shown in Fig. 4 (b).

5. Conclusion and future works

In this paper, the use of co-operative relays for improving the performance of secure wireless communications in the presence of one or more eavesdroppers was studied. Mainly two co-operative schemes were considered: decode-and-forward (DF) and amplify-and-forward (AF). Impacts of path loss, phase fading and shadowing attenuation were taken into consideration. The effect of fading in PHY layer security was formulated analytically and the simulation results were shown for the two co-operative schemes. Using two iterative algorithms: "hill climbing" and "random search" the secrecy rate was improved by taking both relay weights and source power into consideration.

This work can be extended to other co-operative schemes like co-operative jamming (CJ).Also importance can be given to the modifications in the iterative algorithms for a guaranteed result with less execution time and iterations for obtaining the maximum secrecy rate.

References

[1] Hui Suo, Jiafu Wan, Caifeng Zou; Jianqi Liu. Security in the Internet of Things: A Review. Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference , vol.3; no: pp.648-651; 23-25 March 2012
[2] A. D.Wyner. The wire-tap channel. Bell Syst. Tech. J., vol. 54, no. 8,pp. 1355–1387, 1975.
[3] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wiretap channel. IEEE Trans. Inf. Theory, vol. 24, pp. 451–456, Jul. 1978.
[4] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. IEEE Trans. Inf. Theory, Aug. 2007. [Online]
[5] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. IEEE Trans. Inf. Theory, Oct. 2007.
[6] Lun Dong; Zhu Han; Petropulu, A.P.; Poor, H.V. Secure wireless communications via cooperation. Communication, Control, and Computing, 2008 46th Annual Allerton Conference on , vol., no., pp.1132,1138, 23-26 Sept. 2008
[7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Amplify-and-forward based cooperation for secure wireless communications. in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., Taipei, Taiwan, Apr. 2009.
[8] L. Dong, Z. Han, A. Petropulu, and H. V. Poor. Cooperative jamming for wireless physical layer security. in Proc. IEEE Statistical Signal Processing Workshop, Cardiff, Wales, U.K., Aug.–Sep. 2009.
[9] J. N. Laneman, D. N. C. Tse, and G. W.Wornell. Cooperative diversity in wireless networks: Efficient protocols and outage behaviour. IEEE Trans. Inf. Theory, vol. 50, pp. 3062–3080, Dec. 2004.
[10] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity—Part I: System description. IEEE Trans. Commun., vol. 51, no. 11, pp. 1927–1938, Nov. 2003.
[11] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[12] Lun Dong,Zhu Han,Athina P. Petropulu and H.Vincent Poor. Improving Wireless Physical Layer Security via Cooperating Relays. IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 58, NO. 3, MARCH 2010
[13] Goldsmith and Andrea. Wireless communications. Cambridge university press, 2005.